1/5/6 (Item 6 from file: 351)
DIALOG(R)File 351:Derwent WPI

011377311 **Image available**
WPI Acc No: 1997-355218/ **199733**
XRPX Acc No: N97-294553

Interactively managed information providing method for access control of communication service through computer network - involves evaluating propriety of information and not accepting provision of information when effective term of interactive identifier expires

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9146824	A	19970606	JP 95307231	A	19951127	199733	B

Priority Applications (No Type Date): JP 95307231 A 19951127
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9146824	A		8		

Abstract (Basic): JP 9146824 A

The method involves the connection of a server computer (102) which has world wide web to a client computer (101) in a network (103). Information is provided from the client computer to the server computer using a hypertext transfer protocol. A judging unit judges whether an information acquisition demand is generated for the first time. If the demand is generated for the first time, the hypertext of the initial screen with the demand is returned to the client side. During the acquisition demand for an interactive identifier, a detector (411) checks whether the information providing object is available, and if available, then the identifier is formed and registered.

The hypertext with the identifier is returned to the client side. When the object is not available, an access rejection message is returned. When the information acquisition demand is added, the interactive identifier is extracted. The propriety of the information is evaluated based on the formation time of the identifier. When the effective term of the identifier has expired, the provision of information is not accepted by a detector (414).

ADVANTAGE - Avoids provision of inaccurate information because of leakage of identifier. Assures security of stored information.

Dwg.2/9

Title Terms: INTERACT; INFORMATION; METHOD; ACCESS; CONTROL; COMMUNICATE; SERVICE; THROUGH; COMPUTER; NETWORK; EVALUATE; INFORMATION; ACCEPT; PROVISION; INFORMATION; EFFECT; TERM; INTERACT; IDENTIFY; EXPIRE
Index Terms/Additional Words: WWW; HTTP
Derwent Class: T01
International Patent Class (Main): G06F-012/00
International Patent Class (Additional): G06F-003/14; G06F-013/00; G06F-015/00
File Segment: EPI

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－146824

(43)公開日　平成９年(1997)６月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/00	５４７		Ｇ０６Ｆ	12/00	５４７Ｈ
	3/14	３４０			3/14	３４０Ａ
	13/00	３５７			13/00	３５７Ｚ
	15/00	３３０			15/00	３３０Ｚ

審査請求　未請求　請求項の数２　ＯＬ　（全８頁）

(21)出願番号　特願平7－307231

(22)出願日　平成７年(1995)11月27日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　斉藤　典明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　水澤　純一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

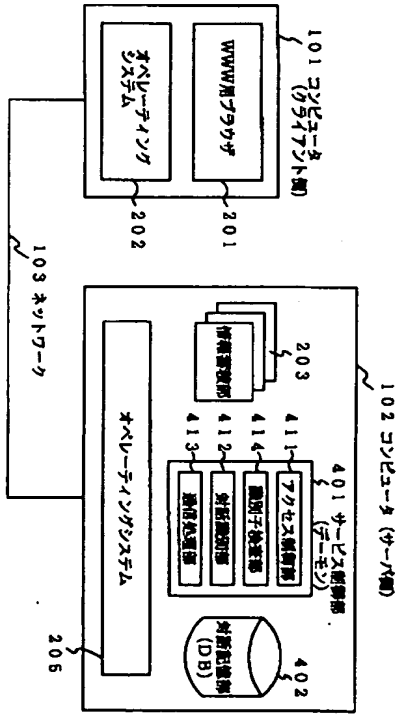
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　対話管理型情報提供方法及び装置

(57)【要約】

【課題】　同一ユーザからの一連のアクセスを識別する対話識別子に有効期限を設け、漏洩した対話識別子により不正な情報提供が行われるのを防止する。

【解決手段】　クライアント１０１は、ユーザからの情報取得要求をネットワーク１０３を通してサーバ１０２に送り、サーバ１０２は該要求で示される情報を情報蓄積部２０３から読み出してクライアント１０１へ返送する。ここで、サーバ１０２のサービス制御部（WWWデーモン）４０１は、情報提供対象ユーザを判別する手段４１１、情報提供対象ユーザに生成日時を付与した対話識別子を発行し、同一ユーザからの一連のアクセスを識別する手段４１２、対話識別子を提供情報に埋め込み該当ユーザに送信する手段４１３、及び、対話識別子を検査し、有効期限が過ぎていると情報提供を認めない手段４１４を有する。



1

【特許請求の範囲】

【請求項1】　情報提供用のWorld－Wide Webを有するサーバコンピュータをコンピュータネットワークでクライアントコンピュータに接続し、HypperText Transfer Protocolにより情報を提供する方法において、

クライアント側からの情報取得要求受信時、初回の情報取得要求か、第2回目以降の情報取得要求かを判定し、

初回の情報取得要求の場合は、対話識別子の取得要求付情報取得要求をもつ初期画面のハイパーテキストをクライアント側に返送し、

第2回目以降の情報取得要求の時、対話識別子の取得要求の場合は、情報提供対象者であるかどうかを判別し、

情報提供対象者の場合、生成日時を明記した対話識別子を生成し、前記対話識別子を登録し、前記対話識別子を付加したハイパーテキストをクライアント側に返送し、

情報提供対象者でない場合、アクセス拒否のメッセージを返送し、

対話識別子の付加された情報取得要求の場合は、該情報取得要求内の対話識別子を抽出し、該対話識別子の生成日時に基づき情報提供の可否の判定を行い、対話識別子の有効期限が切れている場合、情報提供を認めないことを特徴とするコンピュータネットワーク上の対話管理型情報提供方法。

【請求項2】　コンピュータネットワークで接続したクライアントコンピュータに対し、World－Wide Webの情報をHypper Text Transfer Protocolにより提供する対話管理型情報提供装置において、

情報提供対象のユーザと、情報提供対象でないユーザを判別するアクセス制御手段と、

前記情報提供対象のユーザに、生成日時を付与した対話識別子を発行し、一連のアクセスを識別する対話識別手段と、

前記対話識別子の生成日時を検査し、有効期限を過ぎているとき、前記情報提供対象のユーザに情報提供を行わない識別子検査手段と、

前記対話識別子を提供情報に埋め込み、前記提供情報をユーザに送信する通信処理手段とからなることを特徴とする対話管理型情報提供装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータネットワーク上の対話管理型情報提供方法及び装置に関し、詳しくは、ハイパーテキストをコンピュータネットワーク上でユーザに提供するための通信サービスのアクセス制御に関するものである。

【0002】

【従来の技術】従来、ハイパーテキストをコンピュータネットワーク上で、ユーザに対して提供する通信サービスとしWWW（World－Wide Web）が知られており、そのための方法としてＨＴＴＰ（Hypper Text Transfer Protocol）がある。この方法は、不特定多数のユーザへのサービス提供を行うもので、従来は、ユーザのハイパーテキストに対する一連の操作に対して情報取得の要求が生じた時、クライアントコンピュータより、プロトコル、ＩＰアドレス（サーバアドレス）、ポート番号、取得する情報等を、情報取得要求内のＵＲＬ（Uniform ResourceLocator）に設定して、サービス提供元のサーバコンピュータに接続を行い、情報の取得を行っている。

【0003】図6は、従来のこの種のWWWサービスを提供するためのシステム構成例を示したものである。同図において、クライアントコンピュータ１０１とサーバコンピュータ１０２はネットワーク（コンピュータネットワーク）１０３で接続されている。クライアントコンピュータ１０１の内部において、２０１がWWWサービスの提供を受けるための各種ブラウザ、２０２が該コンピュータ１０１を制御するための各種オペレーティングシステムである。また、サーバコンピュータ１０２の内部において、２０３がWWWサービスでユーザに提供するための情報（ハイパーテキストなど）の蓄積部、２０４がWWWサービスを提供するための各種デーモン、２０５が該コンピュータを制御するための各種オペレーティングシステムである。WWW用ブラウザ２０１では、該コンピュータ１０１の入力装置から入力されたユーザからのＵＲＬに従い、ネットワーク上のWWWデーモン２０４に情報取得要求を発行する。情報取得要求を受けたWWWデーモン２０４では、ＵＲＬで示される情報蓄積部２０３内の情報をユーザに転送する。

【0004】図7は、図6のシステム構成におけるクライアントとサーバ間のシーケンスの一例を示したものである。同図において、クライアント側はユーザからの情報取得要求をサーバ（デーモン）側に送り、サーバ側は、要求された情報を情報蓄積部から読み出してクライアント側に返送する。これをユーザから情報取得要求がある毎に繰り返す。なお、サーバは、複数のユーザから複数回、情報提供要求がある場合でも同様の手順で情報を返送する。

【0005】上記WWWの仕組みは、不特定多数のユーザへの情報提供サービスが対象であり、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴により情報の保護等が行えない。

【0006】図8は、従来のWWWサービスを提供するための別のシステム構成例であり、同一ユーザの識別、一連のアクセスの記録、アクセスチェックを可能としたものである。同図において、クライアント側コンピュータ１０１の内部において、２０１がWWWサービスの提供を受けるための各種ブラウザ、２０２が該コンピュータ１０１を制御するための各種オペレーティングシステムである。一方、サーバ側の１０２の内部において、２０３がWWWサービスでユーザに提供するための情報

（ハイパーテキストなど）の蓄積部、４０１が対話管理可能なWWWサービスを提供するためのデーモン（ここでは、サービス制御部という）、４０２が対話管理を行うために必要な情報を蓄積する対話記憶部、２０５が該コンピュータ１０２を制御するための各種オペレーティングシステムである。サービス制御部４０１は、情報提供を行うユーザと提供を行わないユーザを判別するアクセス制御部４１１、情報提供を行うユーザからの一連のアクセスの識別を行う対話識別部４１２、ユーザにメッセージの送信を行う通信処理部４１３からなる。

【０００７】ユーザは、情報を提供するサーバへのアクセスの初期の段階において情報提供対象者であることの認証を受け、情報提供対象者には認証を受けた事を示す識別子が発行され、この識別子がユーザへの提供情報に埋め込まれる。以降、ユーザとサーバの間で取り交わされる一連の情報取得要求と提供情報には、この識別子（対話ＩＤ）が含まれる。

【０００８】図９は、図８のシステムにおけるクライアントとサーバ間のシーケンスの一例を示したものである。クライアント側は、まず（１回目）、ユーザからのＵＲＬに従い、サーバ側に情報取得要求を発行する。サーバ側は、この初回の情報取得要求に対し、情報蓄積部２０３をアクセスし、対話ＩＤ取得要求付情報取得要求のＵＲＬを発行する初期画面をクライアント側に返送する。これを受けて、次に（２回目）、クライアント側は、対話ＩＤ取得要求ＵＲＬの情報取得要求をサーバ側に発行する。サーバ側は、対話ＩＤ取得要求付情報取得要求を判別すると、対話ＩＤを生成し、それを対話記憶部４０２に登録するとともに、要求のあった情報内のＵＲＬに該対話ＩＤを付加してクライアント側に返送する。以後、クライアント側は、ＵＲＬに対話ＩＤを付加して各種情報取得要求をサーバに発行する。サーバ側は、このＵＲＬに付随する対話ＩＤを、対話記憶部４０２を参照してチェックし、正しければ、情報蓄積部２０３をアクセスし、ＵＲＬに対話ＩＤを付加して情報をクライアント側に返送し、対話ＩＤが抽出されないか、該当対話ＩＤが対話記憶部４０２に登録されていない場合は、エラーメッセージなどをクライアント側に返送する。

【０００９】上記方法では、対話識別子の導入により、同一ユーザの識別、ユーザごとの操作履歴の記録、アクセス履歴による情報の保護を行うことができ、不特定多数のユーザを対象とした情報提供サービスにおいて高度のアクセス制御が可能であるが、対話識別子が漏洩した場合、該漏洩した対話識別子により不正な情報提供が行われる問題がある。

【００１０】

【発明が解決しようとする課題】本発明の目的は、ハイパーテキストをコンピュータネットワーク上で不特定多数のユーザに提供するWWWのＨＴＴＰを用いた通信サービスにおいて、同一ユーザからの一連のアクセスを識別する識別子（対話識別子）が漏洩した場合、それにより不正な情報提供が行われるのを防止することにある。

【００１１】

【課題を解決するための手段】本発明は、従来のWWWにおけるＨＴＴＰで利用されるＵＲＬ内の識別子（対話識別子）に、有効期限を設けることを最も主要な特徴とする。

【００１２】ユーザからのアクセスの初期の段階において、サーバは、その対話に対する識別子（対話識別子）を生成し、次回のアクセスに必要となるＵＲＬと対話識別子を付加したハイパーテキストをユーザに提供する。この対話識別子には生成日時が記録されている。クライアントは、転送されてきたハイパーテキスト上の所定の文字をユーザがクリックすることにより、対話識別子とＵＲＬによってサーバにアクセスを行う。サーバはクライアントから送信されてきた情報取得要求の中の対話識別子を解析し、同一ユーザの識別、一連のアクセスの記憶、所定のアクセスのチェックなどを行う。これらのチェックにおいて、サーバは対話識別子に記録されている生成日時が所定の期間より古いものであれば、当該アクセスを無効とする。これにより、対話識別子の漏洩に備えることができるようになる。

【００１３】

【発明の実施の形態】以下、本発明の実施例について図面を参照して説明する。

【００１４】図１は、本発明を適用するコンピュータネットワークの一実施例を示したものである。同図において、１０１はサービスの提供を受けるためにユーザが用いるコンピュータ（クライアントコンピュータ）、１０２はサービスを提供するためのコンピュータ（サーバコンピュータ）、１０３は両者の間で通信サービスを提供するためのネットワークである。クライアントコンピュータ１０１では各種のWWW用ブラウザが動作し、サーバコンピュータ１０２ではWWWサービスを提供する各種デーモンプログラムが動作し、ネットワーク１０３を通してユーザに提供するための情報が蓄積されている。なお、実際には、複数のクライアントコンピュータ１０１がネットワーク１０３によってサーバコンピュータ１０２と接続されている。

【００１５】図２は、本発明におけるシステム構成の一実施例である。同図において、クライアントコンピュータ１０１はWWWサービスの提供を受けるための各種ブラウザ２０１、該コンピュータ１０１を制御するための各種オペレーティングシステム２０２からなる。一方、サーバコンピュータ１０２、WWWサービスにおいてユーザに提供するための情報（ハイパーテキストなど）の蓄積部２０３、対話管理可能なWWWサービスを提供するためのサービス制御部（デーモン）４０１、対話管理を行うために必要な情報を蓄積する対話記憶部４０２、

該コンピュータ１０２を制御するための各種オペレーティングシステム２０５からなる。ここで、サービス制御部４０１は、情報提供を行うユーザと提供を行わないユーザを判別するアクセス制御部４１１、情報提供対象者に発行される識別子を管理する識別子検査部４１４、情報提供を行うユーザからの一連のアクセスの識別を行う対話識別部４１２、ユーザにメッセージの送信を行う通信処理部４１３で構成される。

【００１６】ユーザは、情報を提供するサーバへのアクセスの初期の段階において、アクセス制御部４１１にて情報提供対象者であることの認証を受け、対話識別部４１２にて情報提供対象者には認証を受けたことを示す識別子（対話識別子）が発行され、通信処理部４１３にて、この識別子がユーザへの提供情報に埋め込まれる。以降、ユーザとサーバの間で取り交わされる一連の情報取得要求と提供情報には、この識別子が含まれる。この識別子が識別子検査部４１４にて検査され、一連のアクセスの中である一定期間（例えば１日）以上使用された識別子は廃棄（無効にする）する処理が行われる。

【００１７】図３は、本発明におけるサーバとクライアント間のシーケンスの一例である。これは、ユーザＡの一連のアクセスが１日以上経過すると無効となる例を示したものである図３において、クライアントは、ユーザＡからのＵＲＬに従い、サーバに情報取得要求を発行する（１回目）。サーバは、この初回の情報取得要求に対し、情報蓄積部２０３をアクセスし、ＩＤ取得要求付情報取得要求のＵＲＬを発行する初期画面をクライアントに返送する。これを受けて、クライアントは、対話ＩＤ取得要求付ＵＲＬの情報取得要求をサーバに発行する（２目回）。サーバは、対話ＩＤ取得要求付情報取得要求を判別すると、対話ＩＤを生成し、それを対話記憶部４０２に登録するとともに、要求のあった情報内のＵＲＬに該対話ＩＤを付加してクライアントに返送する。以後、クライアントは、ＵＲＬに対話ＩＤを付加して各種情報取得要求をサーバに発行する（３回目，４回目，・・・）。サーバは、ＵＲＬに付随する対話ＩＤを、対話記憶部４０２を参照してチェックし、正しければ、情報蓄積部２０３をアクセスし、ＵＲＬに対話ＩＤを付加して情報をクライアントに返送する。同時に、サーバは対話ＩＤの有効期限（本例では１日）をチェックし、クライアントから該有効期限の切れた対話ＩＤの付加された情報取得要求が発行されると（ｎ回目）、エラーメッセージをクライアントに返送する。

【００１８】図４は、対話識別子を埋め込んだＵＲＬの一例である。始めのアクセスにおいて、初期画面を得るために用いられる一回目のアクセスのＵＲＬは従来のＷＷＷと同様である。２回目のアクセスにおいて、このＵＲＬにＩＤ取得要求が付加される。３日回以降のアクセスにおいて、クライアントは、各種情報取得要求の他にＩＤ生成時刻（年月日時分秒：例では９５／０５／２２／１１／０１／２７）を明記した対話ＩＤを付加してサーバにアクセスを行う。

【００１９】図５は、図２におけるサーバコンピュータ１０２のサービス制御部４０１のフローチャートの一例である。同図において、破線で囲った部分の符号４１１～４１４は図２のサービス制御部４０１内の該当部分４１１～４１４に対応する。

【００２０】ステップ１００１において、本サーバがクライアントからの要求受付を開始し、ステップ１００２において、ＷＷＷに用いられるブラウザへのＵＲＬの入力により、サーバはクライアントより情報取得要求を取得する。ステップ１００３において、その情報取得要求が初期画面要求（初回アクセス）かどうかを判別し、初期画面要求の場合には、ステップ１００４において、対話識別子（ＩＤ）取得要求のＵＲＬが埋め込まれた初期画面をクライアント（ＷＷＷブラウザ）に送信する。

【００２１】ステップ１００３において情報取得要求が初期画面要求でないと判別された場合には、ステップ１００５において、情報取得要求の中に識別子取得要求があるかを判別し、識別子取得要求である場合には、ステップ１００６において、識別子取得要求内のユーザ情報を元に情報提供対象者であるかどうを判別し、情報提供対象者である場合には、ステップ１００７において対話識別子を生成し、ステップ１００８において、対話識別子とユーザ情報を対話記憶部（ＤＢ）４０２に記録し、ステップ１００９において、提供する情報の中のＵＲＬへ該対話識別を埋め込み、ステップ１０１０において、その対話識別子の埋め込まれた提供情報をＷＷＷブラウザへ送信する。ステップ１００６において、識別子取得要求内のユーザ情報が情報提供対象者でない場合には、ステップ１０１７において、アクセス否拒のメッセージをＷＷＷブラウザへ送信する。

【００２２】ステップ１００５において情報取得要求の中に識別子取得要求がないと判別された場合には、即ち、情報取得要求にすでに対話識別子（ＩＤ）が付加されている場合は、ステップ１０１１において、情報取得要求内の対話識別子を抽出し、ステップ１０１２において、該抽出した対話識別子の有効期限を検査し、有効期限内であれば、ステップ１０１３において、ＤＢ４０２を用い、対話識別子とユーザ情報および情報取得要求により情報提供の可否を判別し、情報提供が許可できる場合には、ステップ１０１４においてＤＢ４０２へアクセス記録を残し、ステップ１０１５において、提供情報中のＵＲＬへ対話識別子を埋め込み、ステップ１０１６において、その情報をＷＷＷブラウザに送信する。一方、ステップ１０１２において抽出した対話識別子の有効期限が切れていると判別された場合には、ステップ１０１７において、アクセス拒否のメッセージがＷＷＷブラウザに送信される。また、ステップ１０１３における判定結果、情報提供が認められない場合にも、ステップ１０

7

１７においてアクセス拒否のメッセージがWWWブラウザに送信される。

【００２３】

【発明の効果】以上説明したように、本発明によれば、一連のアクセスに対する識別子に有効期限を設けることにより、識別子が漏洩した場合においても蓄積情報のセキュリティが確保される効果がある。

【図面の簡単な説明】

【図１】本発明で対象とする通信サービスを提供するためのシステム構成の一例である。

【図２】本発明のサーバコンピュータとクライアントコンピュータのシステム構成の一実施例である。

【図３】本発明におけるサーバとクライアント間のシーケンスの一例である。

【図４】本発明における対話識別子を埋め込んだＵＲＬの一例である。

【図５】図２におけるサービス制御部のフローチャートの一例である。

【図６】従来のWWWサービスを提供するためのシステム構成の一例である。

8

【図７】図６のサーバとクライアントにおけるシーケンスの一例である。

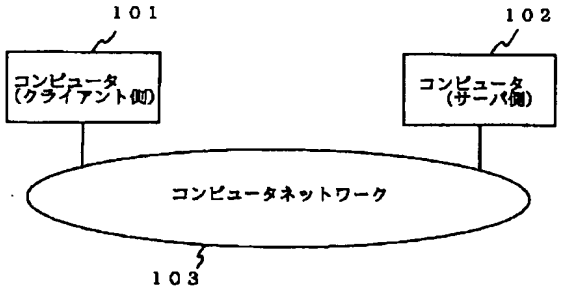
【図８】従来のWWWサービスを提供するためのシステム構成の別の一例である。

【図９】図８のサーバとクライアントにおけるシーケンスの一例である。

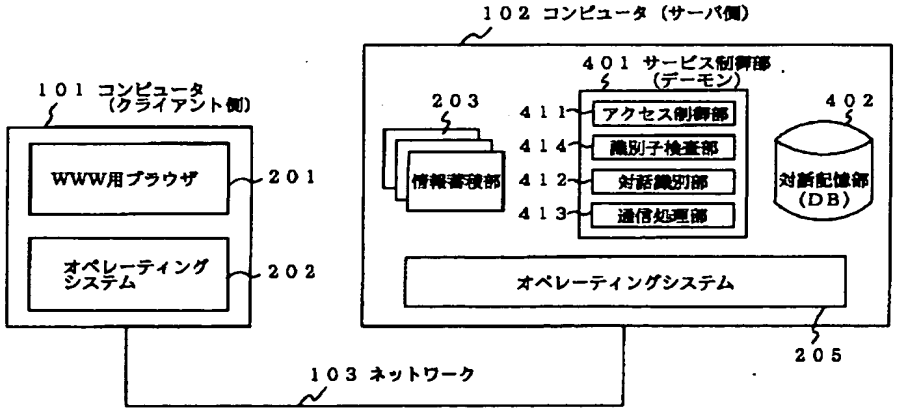
【符号の説明】

１０１　クライアントコンピュータ
１０２　サーバコンピュータ
１０３　ネットワーク
２０１　WWW用ブラウザ
２０２　オペレーティングシステム
２０３　情報蓄積部
２０５　オペレーティングシステム
４０１　サービス制御部
４０２　対話記憶部
４１１　アクセス制御部
４１２　対話識別部
４１３　通信処理部
４１４　識別子検査部

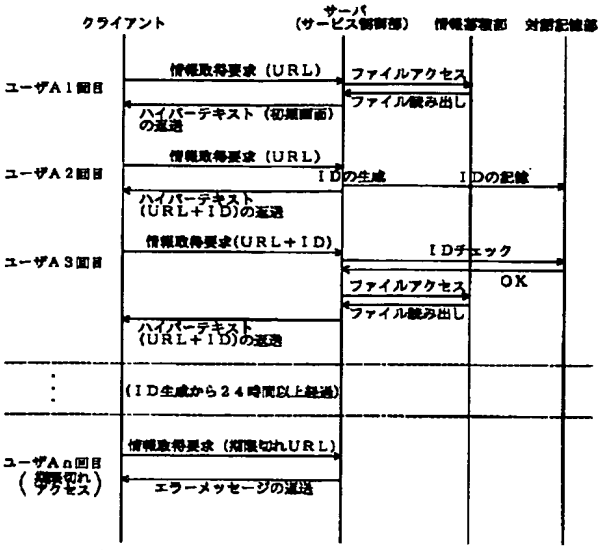
【図１】



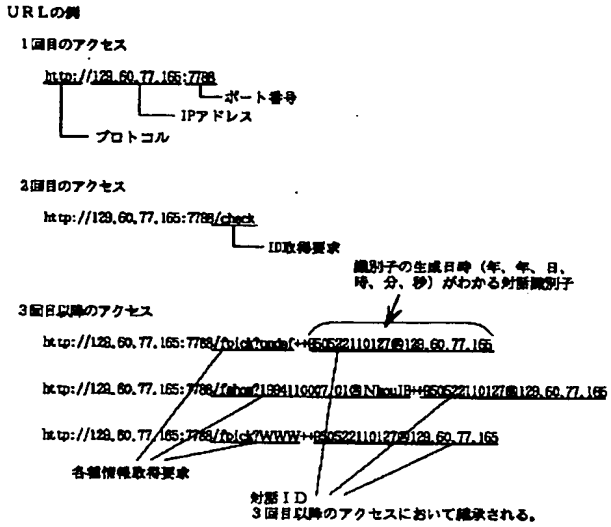
【図２】



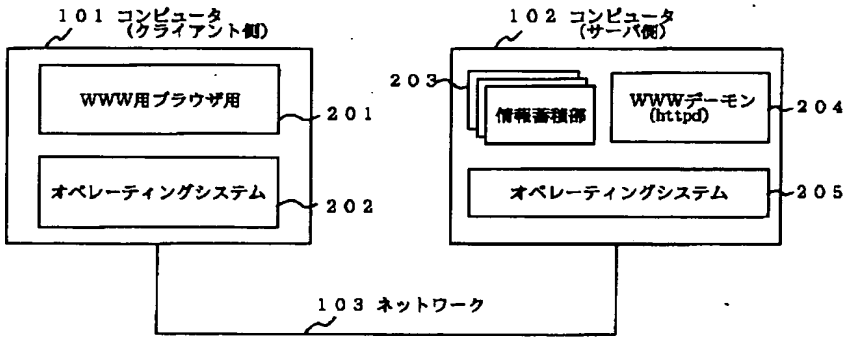
【図３】


クライアント
サーバ
（サービス制御部）
情報蓄積部
対話記憶部
ユーザA１回目
情報取得要求（URL）
ファイルアクセス
ファイル読み出し
ハイパーテキスト（初期画面）の返送
ユーザA２回目
情報取得要求（URL）
IDの生成
IDの記憶
ハイパーテキスト（URL＋ID）の返送
ユーザA３回目
情報取得要求（URL＋ID）
IDチェック
OK
ファイルアクセス
ファイル読み出し
ハイパーテキスト（URL＋ID）の返送
（ID生成から２４時間以上経過）
ユーザAn回目（期限切れアクセス）
情報取得要求（期限切れURL）
エラーメッセージの返送

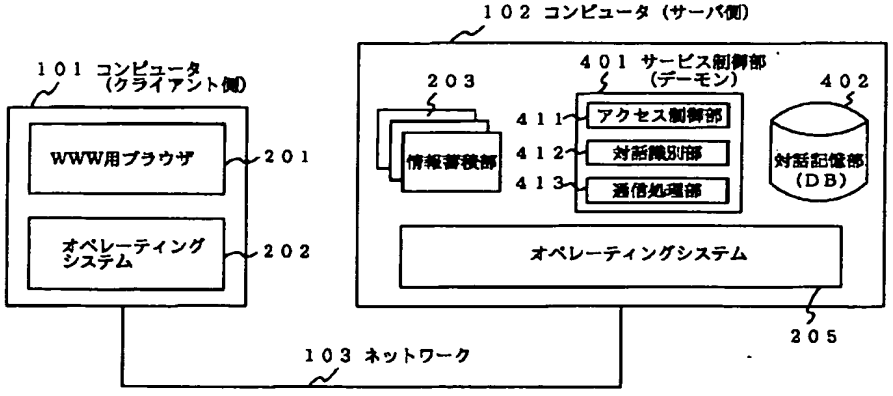
【図４】


URLの例
1回目のアクセス
http://129.60.77.165:7788
ポート番号
IPアドレス
プロトコル
2回目のアクセス
http://129.60.77.165:7788/check
ID取得要求
識別子の生成日時（年、年、日、時、分、秒）がわかる対話識別子
3回目以降のアクセス
各種情報取得要求
対話ID
3回目以降のアクセスにおいて継承される。

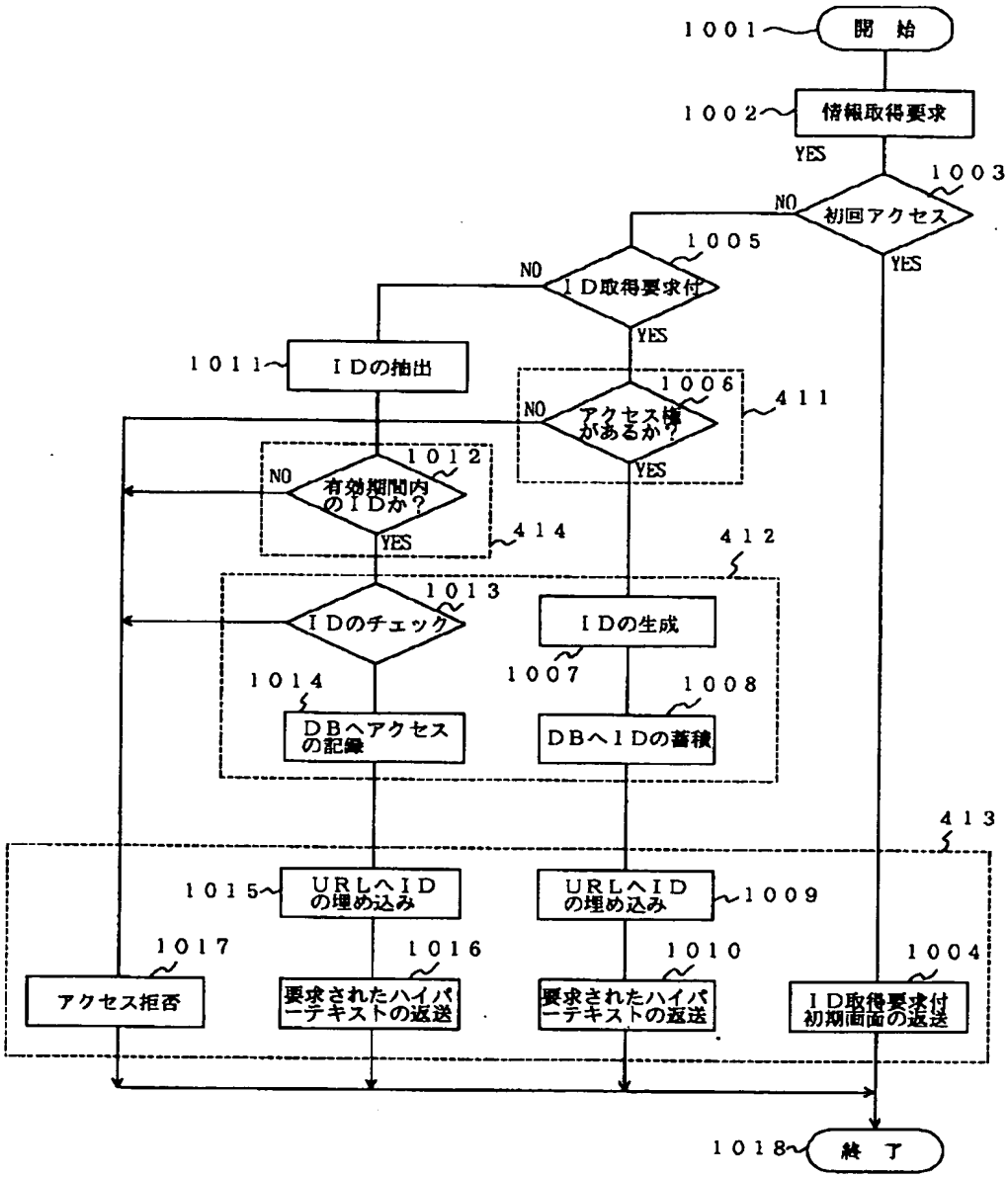
【図６】


101 コンピュータ（クライアント側）
WWW用ブラウザ用
201
オペレーティングシステム
202
102 コンピュータ（サーバ側）
203
情報蓄積部
WWWデーモン（httpd）
204
オペレーティングシステム
205
103 ネットワーク

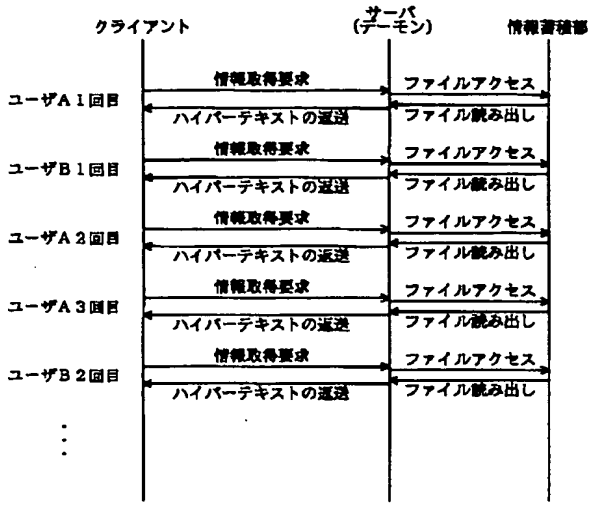
【図８】


102 コンピュータ（サーバ側）
101 コンピュータ（クライアント側）
WWW用ブラウザ
201
オペレーティングシステム
202
203
情報蓄積部
401 サービス制御部（デーモン）
411 アクセス制御部
412 対話識別部
413 通信処理部
402
対話記憶部（DB）
オペレーティングシステム
205
103 ネットワーク

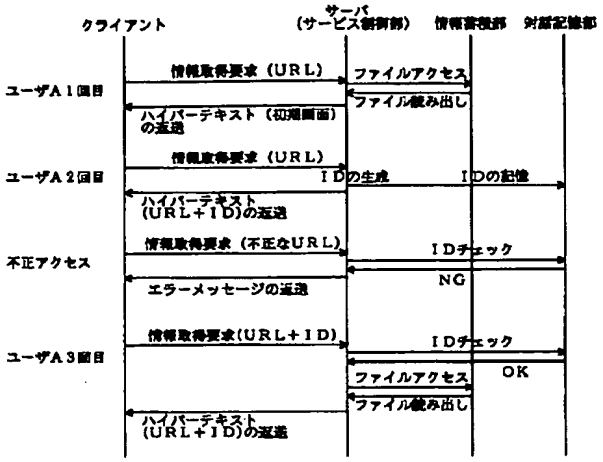
【図５】


１００１
開　始
１００２
情報取得要求
YES
１００３
NO
初回アクセス
YES
１００５
NO
ＩＤ取得要求付
YES
１０１１
ＩＤの抽出
１００６
NO
アクセス権があるか？
４１１
YES
１０１２
NO
有効期間内のＩＤか？
４１４
YES
４１２
１０１３
ＩＤのチェック
ＩＤの生成
１００７
１０１４
１００８
ＤＢへアクセスの記録
ＤＢへＩＤの蓄積
４１３
１０１５
ＵＲＬへＩＤの埋め込み
ＵＲＬへＩＤの埋め込み
１００９
１０１７
１０１６
１０１０
１００４
アクセス拒否
要求されたハイパーテキストの返送
要求されたハイパーテキストの返送
ＩＤ取得要求付初期画面の返送
１０１８
終　了

【図７】


クライアント
サーバ
(デーモン)
情報蓄積部
ユーザＡ１回目
ユーザＢ１回目
ユーザＡ２回目
ユーザＡ３回目
ユーザＢ２回目
情報取得要求
ハイパーテキストの返送
ファイルアクセス
ファイル読み出し

【図９】


クライアント
サーバ
(サービス制御部)
情報蓄積部
対話記憶部
ユーザＡ１回目
ユーザＡ２回目
ユーザＡ３回目
不正アクセス
情報取得要求（URL）
ファイルアクセス
ファイル読み出し
ハイパーテキスト（初期画面）の返送
ＩＤの生成
ＩＤの記憶
ハイパーテキスト(URL＋ＩＤ)の返送
情報取得要求（不正なURL）
ＩＤチェック
NG
エラーメッセージの返送
情報取得要求(URL＋ＩＤ)
OK
ハイパーテキスト(URL＋ＩＤ)の返送